IN THE CLAIMS

1. (currently amended) A method of securely processing a digital signal comprising:

a) generating a public encryption key for use with a first logical circuit and a second logical circuit separate from said first logical circuit;

in a digital media receiving device:

b) accessing an encrypted signal at said first logical circuit;

c) determining a first decryption key for said encrypted signal at said second logical circuit;

d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;

e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;

f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key; and

g) at said first logical circuit, decrypting said encrypted signal using said first decryption key.

2. (original) The method of Claim 1 wherein a) comprises generating said public encryption key using the technique of Diffie-Hellman Key Exchange.

3. (original) The method of Claim 1 wherein d) comprises:

d1) accessing said public encryption key from a first portion of local memory at said second logical circuit;

d2) accessing a computer control program from a second portion of local memory at said second logical circuit; and

d3) executing said computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

4. (original) The method of Claim 1 wherein d) comprises:

d1) accessing said public encryption key from a first portion of local memory at said second logical circuit;

d2) replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program;

d3) accessing said new computer control program from said second portion of local memory; and

d4) executing said new computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

5. (original) The method of Claim 1 wherein f) comprises:

f1) accessing a second decryption key from a first portion of local memory at said first logical circuit;

f2) accessing a computer control program from a second portion of local memory at said first logical circuit; and

f3) executing said computer control program to decrypt said first decryption key using said second decryption key.

6. (original) The method of Claim 1 wherein f) comprises:

f1) accessing a second decryption key from a first portion of local memory at said first logical circuit;

f2) replacing a computer control program stored in a second portion of local memory at said first logical circuit with a new computer control program;

f3) accessing said new computer control program from said second portion of local memory; and

f4) executing said new computer control program at said second logical circuit to decrypt said first decryption key using said second decryption key.

7. (original) The method of Claim 1 wherein said digital signal is substantially compliant with the Motion Pictures Experts Group (MPEG) format.

8-16 (canceled) (election)

17. (currently amended) A system for processing a secure digital signal, comprising:

in a digital media receiving device:

a first logical circuit for decrypting a local encryption key, said first logical circuit comprising a local processor and local memory; and

a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit.

18. (original) The system of Claim 17, further comprising a computer control program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical circuit.

19. (original) The system of Claim 17, further comprising a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory.

20. (original) The system of Claim 17, further configured such that the contents of said local memory cannot be observed from outside of said first logical circuit.

21-25 (canceled) (election)